CROWDSTRIKE

6 Requirements to Minimize External Exposure Risks

Keeping Adversaries in the Dark

CrowdStrike eBook

Adversaries Thrive in the Expanding Attack Surface

It's no secret: The external attack surface is expanding. Digital transformation, remote work, cloud migration and increased reliance on third-party vendors have drastically changed the landscape of the modern economy — ultimately resulting in a plethora of assets that are exposed and vulnerable to cyberattack. In the past, these internet-facing assets were carefully itemized, cleared and managed by a central IT team. Today, most digital assets are located outside the traditional enterprise perimeter — falling outside of IT's visibility and control.

Keeping track of your ever-changing external attack surface might seem like mission impossible — unintentional exposures, misconfigured services and unpatched software represent entry points that attackers can easily exploit to gain access to a company's critical information. According to the CrowdStrike 2023 Threat Hunting Report, more than 20% of all interactive intrusions are associated with the exploitation of public-facing applications.

As a cybersecurity professional, it's not getting any easier. The landscape is one of constant catch-up, dealing with disjointed point products, multiple agents and complex legacy scanners that fall short of efficiently monitoring external attack surfaces. It's an ongoing battle — but not an insurmountable one. By following these six strategic requirements, you'll position yourself to significantly diminish opportunities available to adversaries. This approach not only strengthens your cybersecurity posture but also enables you to proactively protect valuable assets from malicious actors.

Did you know?

400 million
exposed internet-facing assets are detected in a week[1]

76%
of organizations experienced an attack that started with an unknown asset[2]

Top 3
exposed asset categories are Remote Access, DNS and Network Assets[3]

[1] Data from CrowdStrike Falcon® Surface external attack surface management (EASM) module, Dec 2023 - Feb 2024

[2] ESG Research Report: Security Hygiene and Posture Management, April 2023

[3] Data from CrowdStrike Falcon Surface EASM, Dec 2023 - Feb 2024

6 Requirements to Keep Adversaries in the Dark

REQUIREMENT #1:

Prevent sensitive subdomain exposure

Why this matters:

Hostile subdomain takeover allows attackers to seize control of official subdomains, enabling various malicious activities like phishing, content distribution and cookie theft.

Here's what to do:

Monitor your exposed subdomains, make sure all interfaces are secured and require strong authentication. If possible, make sure internet services are connected to a cloud access security broker (CASB) and secured by identity protection with multifactor authentication (MFA) and auditing.

REQUIREMENT #2:

Never allow Remote Desktop Protocol (RDP) connections from outside your organization's networks

Why this matters:

Your organization could suffer from a catastrophic ransomware attack followed by costly data loss. Once adversaries compromise an internet-facing asset, they can move laterally with few restrictions. To put things in perspective, the average adversary breakout time shrunk to 62 minutes in 2023 compared to 84 minutes in 2022[4].

Here's what to do:

Deploy validated and trusted remote access solutions. There are plenty of SaaS and hosted products that offer safe remote access to company resources. Remember, when RDP access is opened to the internet, in most cases, it is not monitored and is highly risky.

[4] CrowdStrike 2024 Global Threat Report

REQUIREMENT #3:

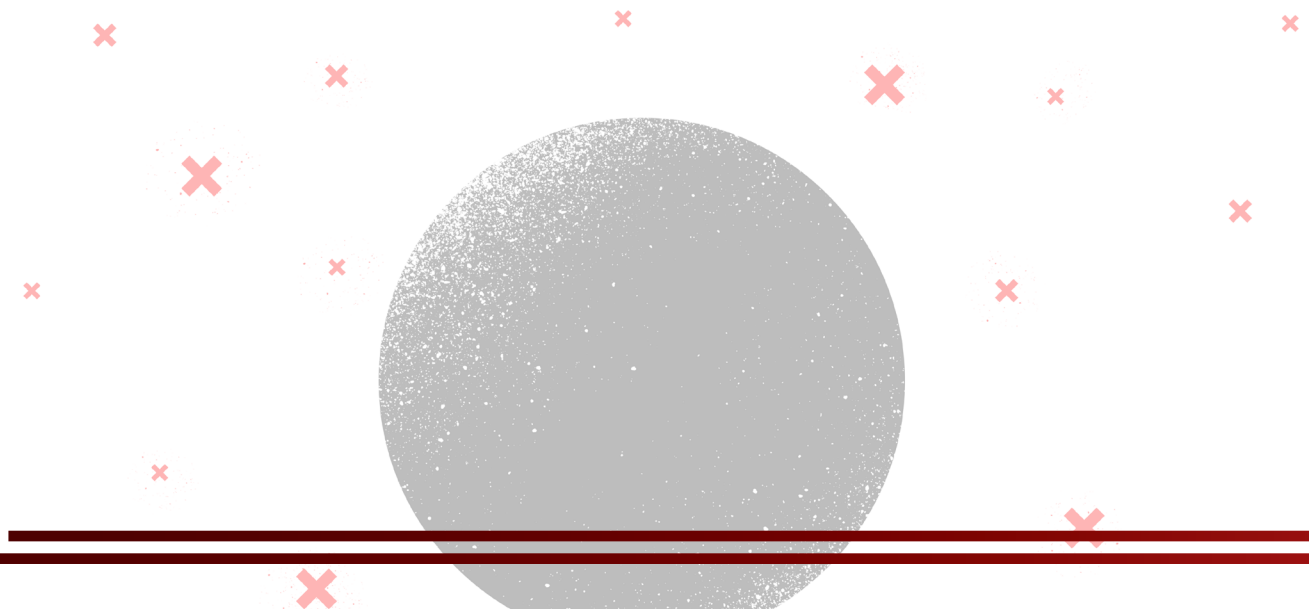
Restrict access to directory listing servers

Why this matters:

Directory listings expose the server to traversal attacks and a large variety of vulnerabilities. Moreover, the web server may contain files that shouldn't be exposed through links on the website.

Here's what to do:

Stand up a server that sits outside of your network perimeter, and install nmap or any other network scanner you are comfortable with. The next step is to get a list of your IP ranges and set up a cron job to scan continuously for open HTTP. Get the logs weekly for every host answering on an HTTP or HTTPS port, and use this list as an input for your web app scanning tool of choice (such as nikto or dirsearch). For any host allowing directory traversal, find the person inside your company who owns or is responsible for this website.



REQUIREMENT #4:

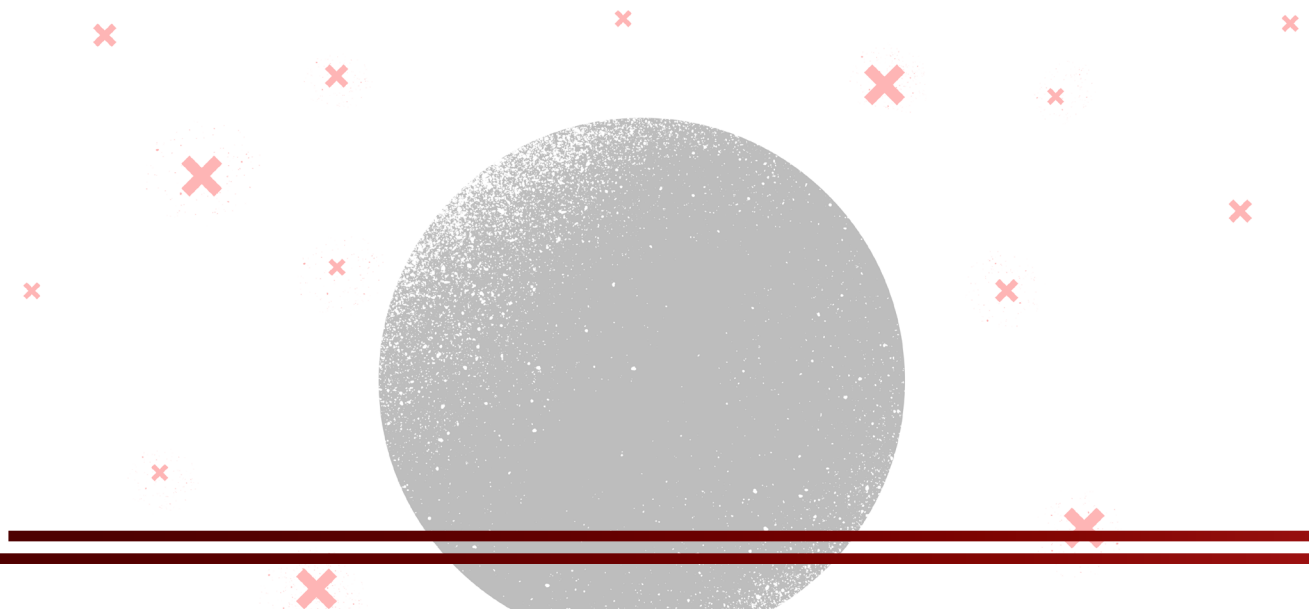
Hide the origin IP address on DNS records

Why this matters:

Your origin server's IP address is where your website or application is actually hosted. If this IP address is exposed, attackers can directly target it with various types of attacks, especially distributed denial of service (DDoS). Moreover, attackers can bypass web application firewall (WAF) deployments, undermining WAF security measures.

Here's what to do:

Begin by reviewing your DNS records, particularly with services like Cloudflare. Confirm that your origin server's IP address isn't directly exposed in these records. Regularly review DNS settings to maintain origin IP address secrecy, and stay updated on any changes from your DNS provider that could affect visibility.



REQUIREMENT #5:

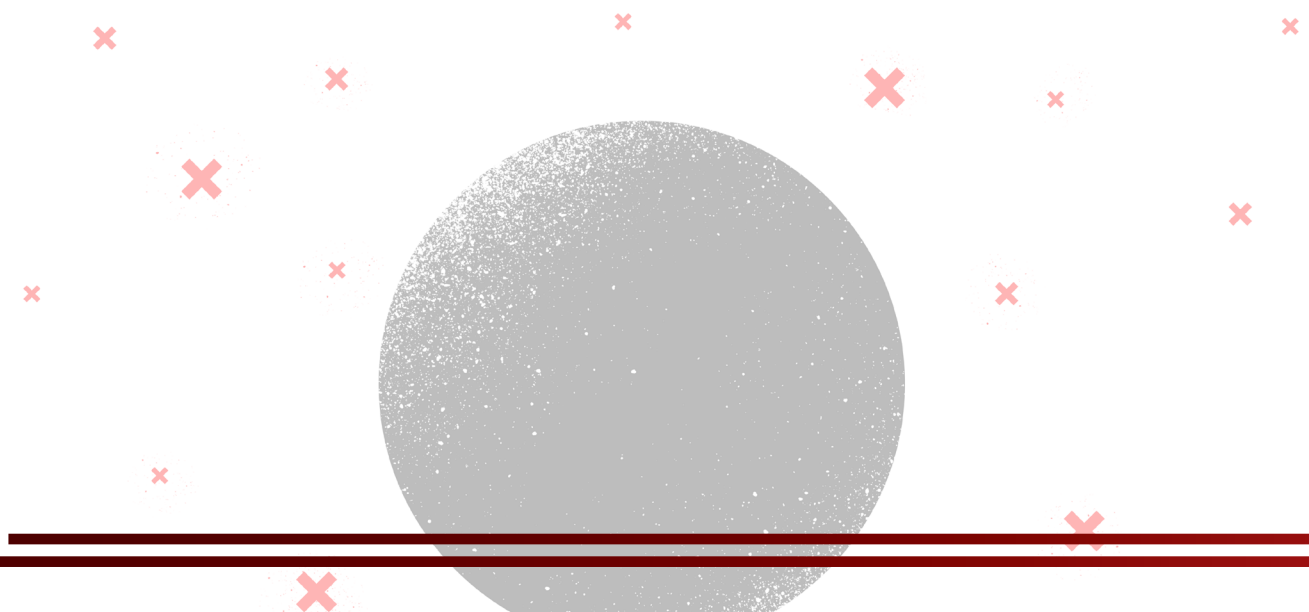
Remove outdated web applications

Why this matters:

Unmaintained services are likely to have multiple vulnerabilities. The longer they stay unmaintained, the higher the probability of one of those vulnerabilities being exploited by an adversary.

Here's what to do:

Build a complete inventory of your company's Internet-facing applications. From this list, decommission any unneeded applications and confirm that the remainder are being regularly patched. This is particularly relevant for open-source software such as WordPress, Joomla, OpenCRM, OpenSSL, Apache and others.



REQUIREMENT #6:

Continuously monitor your attack surface

Why this matters:

Continuous monitoring of your external attack surface isn't just recommended — it's a key security practice. This ongoing vigilance helps spot vulnerable known and unknown assets early, reducing exposure to threats and ensuring regulatory compliance.

Here's what to do:

External attack surface management (EASM) capabilities empower you to proactively identify and mitigate risks in your external-facing assets. However, not all EASM capabilities are equal. When selecting an EASM solution, carefully consider the scanning coverage and frequency, as they directly influence the size and quality of your results. These factors ultimately determine the effectiveness of your EASM in safeguarding your entire attack surface.

These requirements provide an initial advantage in keeping adversaries at bay. But a proactive approach is crucial for robust defense against stealthy attacks. Remember, attackers seek the path of least resistance and are persistent. Shifting from reactive to proactive security is key. Implementing an effective exposure management strategy empowers teams to proactively monitor and secure entire IT landscapes, prioritize critical vulnerabilities and take immediate action in stopping breaches before they happen.

The CrowdStrike Approach to Exposure Management

CrowdStrike Falcon® Exposure Management is an incredibly powerful module delivered as part of the unified, AI-native Falcon platform.

Falcon Exposure Management reduces cyber risk by enabling you to prioritize and proactively remediate vulnerabilities that could lead to a breach. The module combines CrowdStrike's industry-leading threat intelligence with AI-based vulnerability telemetry from the Falcon platform to help you predict attack paths and prioritize risk mitigation actions to stop breaches before they happen.

Complete attack surface visibility: Reduce risk with real-time visibility of all internal assets, external assets and unknown exposures without complex scanning infrastructure.

AI-powered risk prioritization: Proactively stop breaches with analytics-based vulnerability prioritization and predictive attack path mapping sourced from front-line adversary insights.

Consolidate point products with a unified platform: Cut complexity and costs by consolidating EASM, risk-based vulnerability management (RBVM), IT asset management (ITAM) and continuous attack surface management (CASM) tools in an integrated platform, all delivered from a single lightweight agent.

Up to 200%
faster high-risk CVE prioritization with CrowdStrike ExPRT.AI by eliminating manual process and CVSS scoring[5]

Up to 75%
reduction in external attack surface with 24/7 internet monitoring[5]

Up to $200,000
USD annual savings by consolidating vulnerability management point products[5]

Source: Customer assessments

[5] These numbers are projected estimates of average benefits based on recorded metrics provided by customers during pre-sale motions that compare the value of CrowdStrike with the customer's incumbent solution. Actual realized value will depend on the individual customer's module deployment and environment.

Next steps for more information to become a champion in exposure management:

- Schedule a Falcon Exposure Management demo
- Register for a hands-on workshop:
  Empowering Proactive Protection with CrowdStrike Falcon Exposure Management
- See Falcon Exposure Management in action
- Read the Falcon Exposure Management data sheet

About CrowdStrike

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk — endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: We stop breaches.

Follow us: Blog | X | LinkedIn | Facebook | Instagram
Learn more: https://www.crowdstrike.com/